

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 418 486 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.05.2004 Bulletin 2004/20

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **03256947.7**

(22) Date of filing: **04.11.2003**

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT RO SE SI SK TR**
Designated Extension States:
AL LT LV MK

(72) Inventor: **Lee, Woo-hyoung**
Yongin city Kyungki-do (KR)

(74) Representative: **Geary, Stuart Lloyd et al**
Venner, Shipley & Co.,
20 Little Britain
London EC1A 7DH (GB)

(30) Priority: **05.11.2002 KR 2002068261**

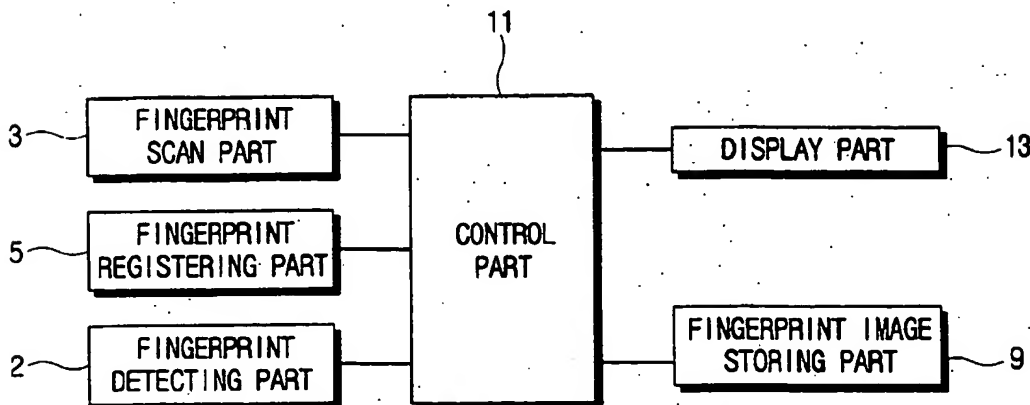
(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.**
Suwon-City, Kyungki-do (KR)

(54) Fingerprint-based authentication apparatus

(57) A security system using fingerprints, including a fingerprint scan part creating a fingerprint image when a finger contacts the fingerprint scan part; a fingerprint image storing part storing representative reference fingerprint images and at least one auxiliary reference fingerprint image for registered users; and a control part determining whether one of the representative refer-

ence fingerprint images matches a first input fingerprint image input through the fingerprint scan part, reading auxiliary reference fingerprint images corresponding to a matching representative reference fingerprint image, and comparing other fingerprint images input after the first input fingerprint image with the auxiliary reference fingerprint images to determine user authentication.

FIG. 2



EP 1 418 486 A2

BEST AVAILABLE COPY

Description

[0001] The present invention relates to an authentication apparatus comprising a memory storing a primary fingerprint of a person, a fingerprint sensor and processing means configured for comparing the output of the fingerprint sensor with the primary fingerprint.

[0002] Security systems has been developed that prevent unauthorized users from gaining access to an area or to information stored in a computer.

[0003] As an example, biometric technologies pre-register and store fingerprints, the shape of the iris or voice signals as identification data.

[0004] A conventional security system using fingerprints pre-registers a plurality of fingerprints using fingerprint recognition apparatus. If a fingerprint of a person desiring access authorization matches a registered fingerprint, access is authorized. Otherwise, access is denied.

[0005] If the conventional security system has a low FAR (False Acceptance Rate) and a high FRR (False Rejection Rate), registered users may be denied access, requiring additional attempts to gain access. However, if the security system has a low FRR, the FAR increases and thus unregistered users may be given access authorization. Thus, a trade-off exists between convenience and security.

[0006] An authentication apparatus according to the present invention is characterised in that the memory stores an auxiliary fingerprint of said person and the processing means is configured for comparing a subsequent output of the sensor with said auxiliary fingerprint in the event of a match in respect of the primary fingerprint.

[0007] Preferably, the memory stores a plurality of auxiliary fingerprints of said person so as to define an ordered list of auxiliary fingerprints and the processing means (11) is configured for comparing subsequent outputs of the sensor with said auxiliary fingerprints in order in the event of a match in respect of the primary fingerprint.

[0008] Preferably, the memory stores primary and auxiliary fingerprints for a plurality of people and the processing means is configured to search for a match between the output of the fingerprint sensor and a primary fingerprint.

[0009] Preferably, the apparatus includes a display and user input means, and the processing means is configured for:

- taking a plurality of sensor outputs and displaying fingerprint images on the display on the basis of said outputs;
- responding to operation of the user input means to store one of said outputs as a primary fingerprint; and
- responding to operation of the user input means to store a plurality of said outputs as auxiliary finger-

prints in a user specified order.

[0010] The apparatus for registering fingerprints may be separate from the apparatus that performs the comparisons.

[0011] An embodiment of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a perspective view illustrating a portable computer with a security system using fingerprints according to the present invention;

Figure 2 is a control block diagram of the security system of Figure 1;

Figure 3 is a flowchart illustrating control of registration of fingerprint images by a security method using fingerprints according to the present invention;

Figure 4 is a flowchart illustrating control of identification of a user by a security method using fingerprints according to the embodiment of the present invention;

Figure 5 illustrates fingerprint images and a selected representative reference fingerprint image for a user according to the present invention;

Figure 6 illustrates auxiliary reference fingerprint images for a user and an input order for comparison of the user's fingerprints, according to the present invention; and

Figure 7 illustrates a table of the representative reference fingerprint image and the ordered auxiliary reference fingerprint images for each registered user according to the present invention.

[0012] Referring to Figure 1, a portable computer 1 includes a system body 10 and a liquid crystal display (LCD) part 15 joined to the system body 10. The system body 10 includes a keyboard part 7, a fingerprint detecting part 2, having multiple contact sensors, and a touch pad 4.

[0013] The security system using fingerprints is implemented by a security program for user authentication. Referring to Figure 2, the security system includes a fingerprint scan part 3 for generating an image on the basis of a detection signal output from the fingerprint detecting part 2, a fingerprint image storing part 9 for storing, for each user, a representative reference fingerprint image and at least one auxiliary reference fingerprint image and a fingerprint registering part 5 for sequentially receiving multiple unregistered images of fingerprints, selecting and ordering one or more of the images as auxiliary reference fingerprint images, and then storing the multiple images in the fingerprint image storing part 9. When a representative reference fingerprint image matches a fingerprint image, input using the fingerprint detecting part 2, a control part 11 reads corresponding auxiliary reference fingerprint images of the user associated with the representative reference fingerprint im-

age, and then compares each auxiliary reference fingerprint image with additional fingerprint images input by the user requesting access authorization to determine whether the user is authenticated. A display part 13 displays whether the user is authenticated and can be implemented using the LCD part 15.

[0014] When a user initially registers fingerprint images, the fingerprint registering part 5 provides an order value between 0 and 9 to the fingerprint images supplied from the fingerprint scan part 3 to correspond to each of the user's ten fingers that contact the fingerprint detecting part 2 sequentially from left to right and then stores the fingerprint images in the fingerprint image storing part 9 according to a user identification (ID). The fingerprint registering part 5 then displays a screen 20 for the user to set the representative reference fingerprint image (refer to Figure 5), described below, and a screen 30 for setting the auxiliary reference fingerprint images and the input order thereof (refer to Figure 6) described below. The fingerprint registering part 5 then stores the input order information, which includes order values for the representative reference fingerprint images, and the auxiliary reference fingerprint image images, in the fingerprint image storing part 9.

[0015] Thus, the control part 11 compares an input fingerprint image from the fingerprint scan part 3 for a user requesting access, with the representative reference fingerprint images and, if a match occurs, corresponding auxiliary reference fingerprint images and the comparison input order information are read from the fingerprint image storing part 9. The user requesting access then inputs additional fingerprint images. The control part 11 determines whether to authenticate a user by analyzing whether the additional fingerprint images are input according to the input order information of the auxiliary reference fingerprint images.

[0016] Referring to Figure 3, multiple fingerprint images of a user are scanned at S1 in a specific order and then input. The fingerprint registering part 5 provides an order value at S3 to the fingerprint images sequentially input and then stores the fingerprint images in the fingerprint image storing part 9. The screen 20 for setting the representative reference fingerprint image (refer to Figure 5) is displayed at S5 on the display part 13. A fingerprint image selected by the user is then set at S7 as a representative reference fingerprint image and stored. The screen 30 for setting the auxiliary reference fingerprint images and the input order thereof (refer to Figure 6) is displayed at S9 to allow the user to select multiple auxiliary reference fingerprint images with a specific order. At this point, the fingerprint registering part 5 stores at S11 the auxiliary reference fingerprint images and the order values thereof in the fingerprint image storing part 9 as the input order information.

[0017] Referring to Figure 4, to authenticate a user at S13, the control part 11 receives a first input fingerprint image at S15 and then compares at S17 the first input fingerprint image with the multiple registered represent-

ative reference fingerprint images. The control part 11 determines at S19 whether one of the representative reference fingerprint image matches the input fingerprint image and then, when a representative reference fingerprint image matches the input fingerprint image, reads at S21 the auxiliary reference fingerprint images corresponding to the matching representative reference fingerprint image. When there are, for example, four auxiliary reference fingerprint images, then when second, third, and fourth fingerprint images are input through the fingerprint scan part 3, the control part 11 determines at S23 through S35 whether the fingerprint images are input in an order corresponding to the input order information stored in the fingerprint image storing part 9, and then determines whether the user is authenticated at S35. When the input fingerprint image is compared with the representative reference fingerprint images at S19 and is not coincident with the representative reference fingerprint images, an error message is displayed by the display part 13 at S20. In determining whether the second through fourth fingerprint images, input through the fingerprint scan part 3, are input in the correct order at S25, S29 and S33, if one of the second through fourth fingerprint images is not correctly input, the display part 13 displays an error message at S26, S30 and S34.

[0018] After the multiple unregistered fingerprint images are input, as shown in Figure 5, the screen 20 for setting the representative reference fingerprint image, which displays the multiple fingerprint images for each of a user's fingers with the specific sequential order values, is displayed on the display part 13. The screen 30 for setting the auxiliary reference fingerprint images and the input order thereof is displayed after the user selects the representative reference fingerprint image. The fingerprint images to be used as the auxiliary reference fingerprint images are selected sequentially and the order of the selected fingerprint images is stored in the fingerprint image storing part 9 with the representative reference fingerprint image as the input order information. The selected representative reference fingerprint image, and auxiliary reference fingerprint images and the input order thereof are displayed for each registered user in the table 40 shown in Figure 7 with an ID for each registered user.

[0019] In the above embodiment, the fingers of both hands of a user are scanned through the fingerprint detecting part 2 in order and order values are assigned to register the fingerprint images. Alternatively, by using multiple fingerprint input keys having respective fingerprint sensor parts and with assigned order values, a user can combine secret numbers with the fingerprint images to make a secret code.

[0020] In the security system of the present invention that allows multiple fingerprints to be registered, an input fingerprint image is compared with multiple stored representative reference fingerprint images, and then stored auxiliary reference fingerprint images corre-

sponding to a representative reference fingerprint image matching the input fingerprint image are compared to additional input fingerprint images to provide user authentication that is fast and convenient.

[0021] As described above, according to the present invention, a system and method using fingerprints is provided to enable fast user authentication by comparing a first input fingerprint image with multiple stored representative reference fingerprint images and, if a match occurs, then sequentially performing a comparison for subsequently input fingerprint images with stored auxiliary reference fingerprint images that correspond to the matching representative reference fingerprint image.

Claims

1. An authentication apparatus comprising:

a memory (9) storing a primary fingerprint of a person;
a fingerprint sensor (3); and
processing means (11) configured for comparing the output of the fingerprint sensor with the primary fingerprint,

characterised in that the memory (9) stores an auxiliary fingerprint of said person and the processing means is configured for comparing a subsequent output of the sensor (3) with said auxiliary fingerprint in the event of a match in respect of the primary fingerprint.

2. An apparatus according to claim 1, wherein the memory (9) stores a plurality of auxiliary fingerprints of said person so as to define an ordered list of auxiliary fingerprints and the processing means (11) is configured for comparing subsequent outputs of the sensor with said auxiliary fingerprints in order in the event of a match in respect of the primary fingerprint.

3. An apparatus according to claim 1 or 2, wherein the memory (9) stores primary and auxiliary fingerprints for a plurality of people and the processing means (11) is configured to search for a match between the output of the fingerprint sensor and a primary fingerprint.

4. An apparatus according to claim 2, including a display (13) and user input means, wherein the processing means (11) is configured for:

taking a plurality of sensor outputs and displaying fingerprint images on the display (13) on the basis of said outputs;
responding to operation of the user input means to store one of said outputs as a primary

fingerprint; and

responding to operation of the user input means to store a plurality of said outputs as auxiliary fingerprints in a user specified order.

5. A security system using fingerprints, comprising:

a fingerprint scan part creating a fingerprint image when a finger contacts the fingerprint scan part;

a fingerprint image storing part storing representative reference fingerprint images and at least one auxiliary reference fingerprint image for registered users; and

a control part determining whether one of the representative reference fingerprint images matches a first input fingerprint image input through the fingerprint scan part, reading auxiliary reference fingerprint images corresponding to a matching representative reference fingerprint image, and comparing other fingerprint images input after the first input fingerprint image with the auxiliary reference fingerprint images to determine user authentication.

6. The security system using fingerprints according to claim 5, wherein the control part displays an error message when the first input fingerprint image does not match any of the representative reference fingerprint images in the fingerprint image storing part.

7. The security system using fingerprints according to claim 6, further comprising a fingerprint registering part sequentially storing fingerprint images input through the fingerprint scan part by an unregistered user in the fingerprint image storing part, and displaying the stored fingerprint images of the unregistered user for the unregistered user to select one of the stored fingerprint images as the representative reference fingerprint image.

8. The security system using fingerprints according to claim 6, wherein the fingerprint registering part assigns sequential order values to the unregistered fingerprint images input through the fingerprint scan part and stores the sequential order values with the input fingerprint images of the unregistered user in the fingerprint image storing part.

9. The security system using fingerprints according to claim 7, wherein the fingerprint scan part comprises multiple fingerprint input keys having order values sequentially selected by the unregistered user; and the fingerprint registering part stores a combination of input fingerprint images contacting the fingerprint input keys selected by the unregistered user and the order values in the fingerprint image storing part.

10. The security system using fingerprints according to claim 8, wherein

the fingerprint registering part displays a screen to set the input order of the auxiliary reference fingerprint images; and

the control part stores the input order of the auxiliary reference fingerprint images in the fingerprint image storing part.

11. A security method using fingerprints, comprising:

storing representative reference fingerprint images and at least one auxiliary reference fingerprint image, according to registered users; receiving a first input fingerprint image for authentication of a user; determining whether one of the stored representative reference fingerprint images matches the first input fingerprint image; reading auxiliary reference fingerprint images corresponding to a matching representative reference fingerprint image; receiving additional fingerprint images sequentially input by the user; and determining whether the user is authenticated by respectively comparing the additional input fingerprint images with the corresponding auxiliary reference fingerprint images.

12. The security method using fingerprints according to claim 11, further comprising displaying an error message when the first input fingerprint image does not match any of the representative reference fingerprint images.

13. The security method using fingerprints according to claim 12, further comprising:

receiving fingerprint images of an unregistered user; and assigning order values to the fingerprint images sequentially input by the unregistered user, and storing the order values with the input fingerprint images.

14. The security method using fingerprints according to claim 13, further comprising displaying a screen for the unregistered user to select one of the stored representative reference fingerprint images as the representative reference fingerprint image.

15. The security method using fingerprints according to claim 14, further comprising:

displaying a screen to select and assign order values to the auxiliary reference fingerprint images; and storing the selected auxiliary reference finger-

print image and the order values with the selected representative reference fingerprint image.

16. The security method using fingerprints according to claim 12, further comprising:

selecting sequentially two or more fingerprint input keys having order values selected by the unregistered user; storing a combination of fingerprint images input through the selected fingerprint input keys and the order values; and determining authentication of a user requesting authentication by determining whether an order of the fingerprint images input through the fingerprint input keys matches the selected order values and whether the input fingerprint images match the stored auxiliary reference fingerprint images.

17. A fingerprint security method, comprising:

receiving and storing fingerprint images for each finger of one or more unregistered users; displaying the stored fingerprint images for the unregistered user to select one of the stored fingerprint images as a representative reference fingerprint image; displaying the stored fingerprint images for the unregistered user to select and order one or more of the stored fingerprint images as ordered auxiliary reference fingerprint images; registering the user with the corresponding representative reference fingerprint image and the auxiliary reference fingerprint images; receiving a first fingerprint image from a user to be authenticated; determining whether the first fingerprint image matches any of a plurality of stored representative reference fingerprint images for a plurality of registered users; receiving, when the first fingerprint image matches one of the stored representative reference fingerprint images, additional fingerprint images sequentially input by the user to be authenticated; and determining whether each of the additional fingerprint images matches auxiliary reference fingerprint images corresponding to the representative reference fingerprint image that matches the first fingerprint image, and whether the additional fingerprint images are input according to the selected order of the corresponding auxiliary reference fingerprint images.

18. The fingerprint security method according to claim

17, further comprising displaying an error message when the first input fingerprint image does not match any of the representative reference fingerprint images.

5

10

15

20

25

30

35

40

45

50

55

FIG. 1

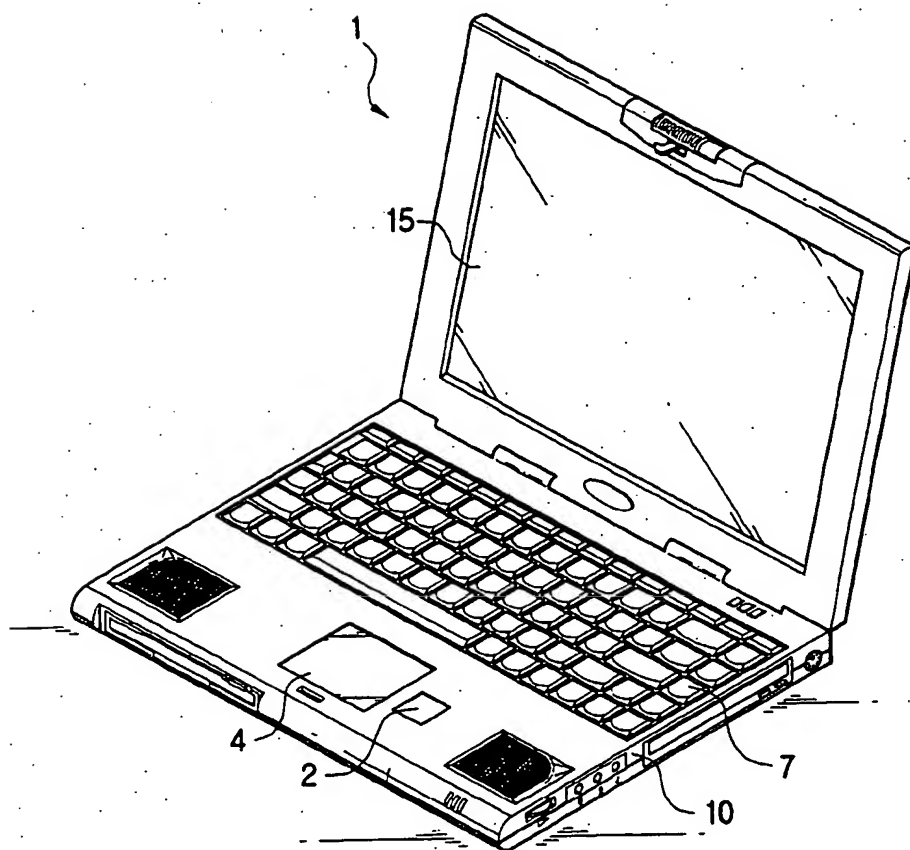


FIG. 2

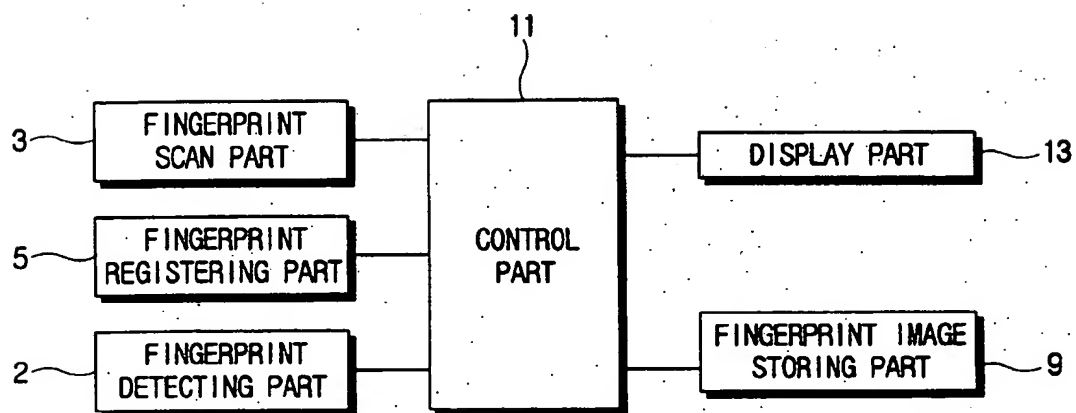


FIG. 3

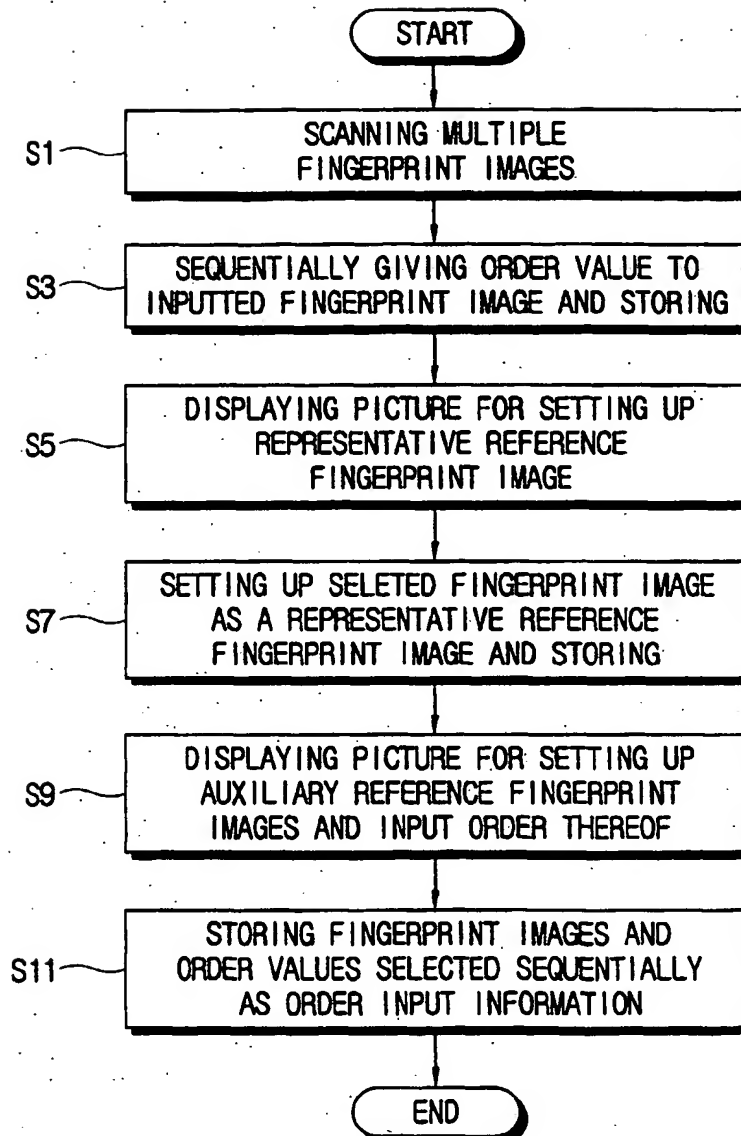


FIG. 4

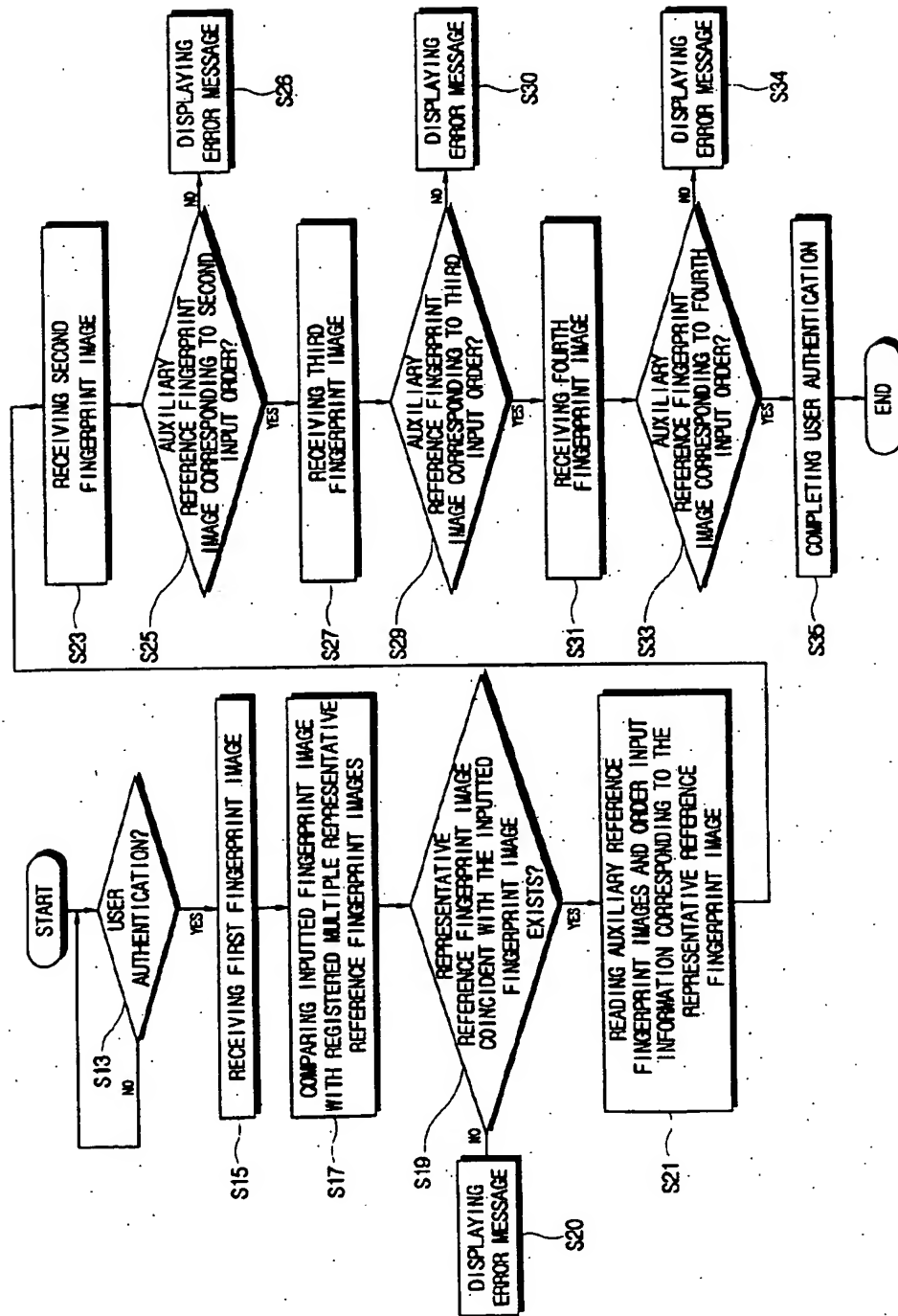


FIG. 5

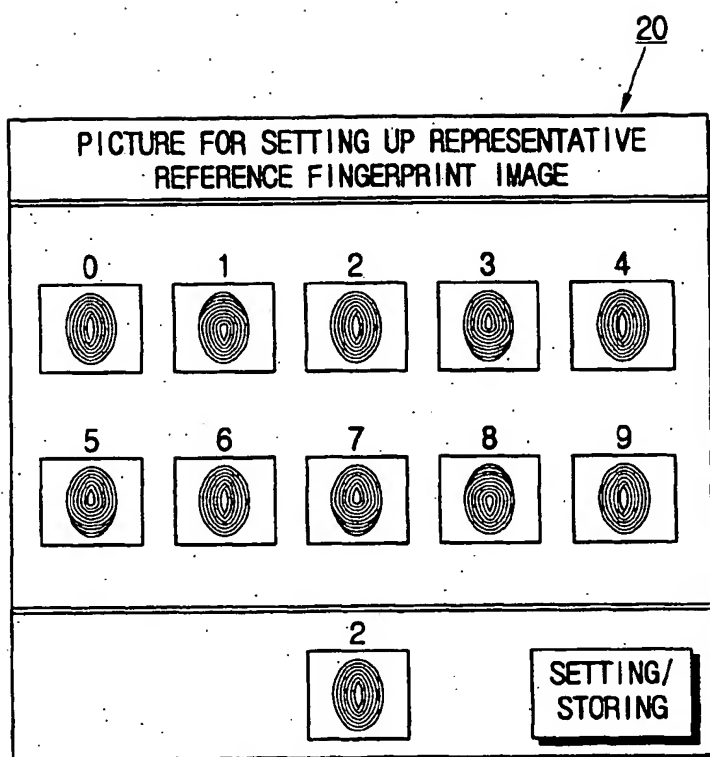


FIG. 6

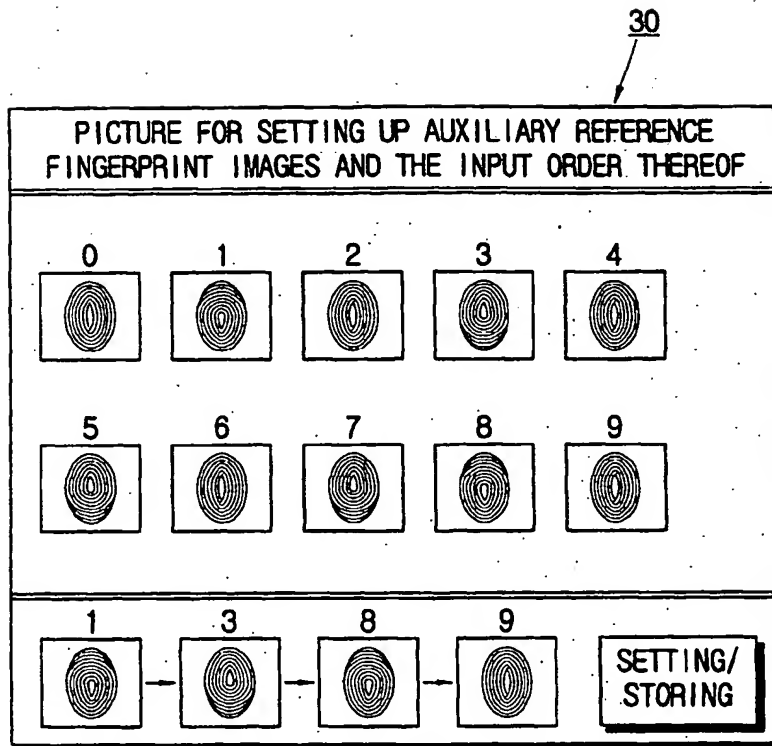

















FIG. 7

40

ID	REPRESENTATIVE REFERENCE FINGERPRINT IMAGE	INPUT ORDER OF AUXILIARY REFERENCE FINGERPRINT IMAGES
AAA	2 	1 → 3 → 8 → 9  →  →  → 
BBB	3 	2 → 5 → 4 → 7  →  →  → 
CCC	4 	4 → 9 → 0 → 5  →  →  → 
⋮	⋮	⋮

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.